routines of a control program stored in a memory **412**. The control program may also be stored separately on a computer-readable medium. Program code instructions are fetched from the memory **412** and are loaded to the control unit of the processing unit **410** in order to perform the processing steps of the above functionalities of FIGS. **2** to **5**, which may be implemented as the above-mentioned software routines. The processing steps may be performed on the basis of input data DI and may generate output data DO. The input data DI may correspond to the authentication parameters mentioned in the above equations for calculating the GBA key Ks or the digest-GBA-response parameter, and the output data DO may correspond to the GBA key Ks or the digest-GBA-response parameter.

**[0089]** Consequently, the above embodiments may be implemented as a computer program product comprising code means for generating each individual step of the signaling procedures of FIGS. **3** to **5** for the respective authentication entity when run on a computer device or data processor of the respective authentication entity at the UE **10** or the BSF **20** or any corresponding terminal device or network entity.

**[0090]** In summary, a method, apparatus, and computer program product have been described, in which a password-based digest access authentication procedure is used for performing authentication between a client and a server, wherein the authentication procedure is secured by at least one of modifying a digest-response parameter with a user password and generating a bootstrapped key based on the user password and at least one fresh parameter not used in a previous protocol run between the client and the server.

**[0091]** It is apparent that the invention can easily be extended to any service and network environment (fixed and wireless), where a password-based digest access authentication procedure is used. It can be used in connection with any authentication between a client and a server. More specifically, the BSF **20** may as well be any authentication authorization and accounting (AAA) server or any other attachment node with a BSF or AAA functionality. The embodiments may thus vary within the scope of the attached claims.

**1**. An apparatus, comprising:

one or more processors; and

one or more memories including computer program code, the one or more memories and the computer program code configured, with the one or more processors, to cause the apparatus to perform at least the following:

a) authenticate at a bootstrapping server a user device to the bootstrapping server using a digest access authentication procedure based on a password;

b) establish at the bootstrapping server a shared key between the user device and the bootstrapping server;

c) secure the authentication procedure at the bootstrapping server using a key derivation function, wherein the key derivation function calculates a modified digest response parameter; and

d) generate at the bootstrapping server a bootstrapped key to serve as the shared key based on the digest response parameter, wherein at the bootstrapping server the digest response parameter is determined to have not been used in a previous protocol run between the user device and the bootstrapping server.

**2**. The apparatus according to claim **1**, wherein the key derivation function uses the user password and the digest response parameter as input values, where the digest response parameter is calculated using a hash function which uses a nonce as an input.

**3**. The apparatus according to claim **2**, further comprising generating the bootstrapped key by applying a second hash function to the digest response parameter and an arbitrary string parameter.

**4**. The apparatus according to claim **1**, further comprising, at the bootstrapping server, modifying interfaces transmitted from the bootstrapping server to the user device and to a subscriber database, while leaving interfaces between the bootstrapping server and the network application function and between the network application function and the user device in conformity with a specification underlying the digest access authentication procedure.

**5**. The apparatus according to claim **1**, further comprising modifying the digest response parameter by applying a hash function to a user name, the user password, and a nonce value.

**6**. The apparatus according to claim **1**, wherein the bootstrapped key is available to further derive security keys for use between the user device and a network application function in a derivation subsequent to the generation of the bootstrapped key.

**7**. The apparatus according to claim **1**, wherein the digest response parameter comprises nonce values exchanged between the user device and the server.

**8**. The apparatus according to claim **1**, wherein the digest response parameter comprises a server-specific random number.

**9**. A generic bootstrapping architecture method, the method comprising:

a) authenticating, at a bootstrapping server, a user device using a digest access authentication procedure based on a random number and a password;

b) establishing, at the bootstrapping server, a shared key;

c) securing the authentication procedure, at the bootstrapping server, using a key derivation function, wherein the key derivation function calculates a modified digest response parameter; and

d) generating, at the bootstrapping server, a bootstrapped key to serve as the shared key based on the digest response parameter, wherein at the bootstrapping server the digest response parameter is determined to have not been used in a previous protocol run.

**10**. A computer program product stored on a non-transitory computer readable medium and comprising:

code for producing the steps of:

a) authenticating at a bootstrapping server a user device to the bootstrapping server using a digest access authentication procedure based on a password;

b) establishing at the bootstrapping server a shared key between the user device and the bootstrapping server;

c) securing the authentication procedure at the bootstrapping server using a key derivation function, wherein the key derivation function calculates a modified digest response parameter; and

d) generating at the bootstrapping server a bootstrapped key to serve as the shared key based on the digest response parameter, wherein at the bootstrapping server the digest response parameter is determined to